DEVI AHILYA VISHWAVIDYALAYA, INDORE

IT Policy

2019


उन्नत समाज समृद्ध राष्ट्र

“ We Should not Give Up

and We Should not allow

the Problems to Defeat Us ”

- A.P.J. Abdul Kalam

Table of Contents

		Page No.
1.	*Foreword*	1
2.	*Preamble*	2
3.	*To Whom It Applies to*	4
4.	*IT Services*	5
5.	*IT Hardware and Software Installation*	6
6.	*IT Centre Interface*	10
7.	*Open Source Resource Usage*	10
8.	*Network and Information Security*	11
9.	*Software Asset Management*	15
10.	*Green Computing*	16
11.	*Concluding Remarks*	17

IT Policy
2019

Foreword ....

Devi Ahilya University recognizes the vital role of Information Technology in the University's missions and related administrative activities as well as its importance in an academic domain of preserving information in digital forms. The University provides its faculty, staff and students a network eco system to facilitate the missions of the University, which includes instruction, research, service and administration. University has recently extended its network to all hostels to provide wired and wireless access to Internet.

The University framed its IT Policy first time in year 2014 describing its values for using its computing facilities including computer hardware, software, e-mail, intranet and Internet access collectively known as "Information Technology (IT) facilities". The IT Policy 2019 extends this domain by including how effectively the existing IT infrastructure should be used to provide various services to its users. It also describes future road map for providing services and upgradation of IT infrastructure. In addition to all points from previous policy document, this document covers about various enhanced services planned for its users. These services include implementing University ERP system and establish data resource center for its e-Governance goals, create test bed facilities for experimental research in areas like wireless sensor networks, multimedia networks, IoT and security, and pervasive computing, High performance computing facilities for research activities.

Preamble

Now a day, Intranet and Internet systems become the integral part in educational institutions. Several Online services made available to academic fraternity through these systems. Realizing the importance of these systems, DAVV took initiative in year 1998 to establish basic network and IT infrastructure in university campus. University completed first phase of campus wide network development in year 2000 by covering all UTDs of Takshashila campus. The second and third phase of IT infrastructure development accomplished the networking of Nalanda campus and IET campus subsequently in years 2002 and 2003. Recently in years 2016-18 the network services have been extended to all hostels of the University. Both campuses and hostels have been Wi-Fi enabled. Over these years, not only active users of the network facilities have increased many folds but also the web-based applications have increased.

Presently, the university has about 5000 network connections and 10000+ users covering more than thirty-eight buildings and twelve hostels. IT Centre has been given the responsibility of running the university's intranet & Internet services. University is providing Internet services to its students, faculty and staff on using 1 Gbps Internet lease line connectivity of National Knowledge Network (NKN). This connectivity along with developed IT infrastructure has been successfully used in conducting several online interactive workshops held under NMEICT. These workshops were remotely conducted by IITs and IIITs in different domains on various subjects. Virtual class rooms have been set up in two departments of the University.

University is running several in-house IT and network support services such as email and web service, Proxy and Firewall services for access control, LDAP as authentication service, DNS for name to IP resolution. These services are centrally managed by IT Centre. The University provides its information technology resources to a large and varied group, including faculty, staff, and students. All users are expected to use these resources in an efficient and ethical manner.

Several University e-Governance services are also made available through University web portal. These services are online admissions, results, registrations, various forms and fess submission. All these services are user and student centric.

The uncontrolled and free web access gives rise to activities that obstruct the network speed and uniform access to all users. This also poses following problems, which need to be addressed:

- Intermittent surfing, affecting quality of work.
- Bandwidth chocking due to heavy downloads.
- When users are given free access to the Internet, non-critical repeated downloads may clog the traffic, resulting in poor Quality of service (QoS) thereby affecting critical users and application performance.
- Viruses spread very fast over unsecure LANs through intranet and exploit vulnerabilities of operating systems that result into data loss or break into service. Containing a virus once it spreads through the network becomes hard to remove. Several man hours are needed in making network operational and safe again.
- IT Centre has taken utmost care in protecting network from attacks and vulnerabilities. Firewall and content filtering software and hardware based UTM system already been deployed in the network along with powerful enterprise level antivirus solution.

Clearly defined IT policies are strongly needed to convince users about the steps that are taken for managing the network. Policies and guidelines form the foundation of the Institution's IT security program and often required to mention at the time of IT audit or any litigation against Institution.

In view of above, Devi Ahilya Vishwavidyalaya, Indore proposes its IT Policy, that will also work as course of action for using University's computing facilities including computer hardware, software, email, intranet and internet access collectively called as "Information Technology (IT) facilities". The DAVV IT policy shall articulate

university's values, principles, strategies and positions relative to a broad IT topic. Further, it will set direction and provide information about acceptable actions and prohibited actions.

To Whom it Applies to

University IT Policy applies to all University Teaching Departments, Centers, Libraries, Hostels and computer centers wherever the network facility is provided by the University. Computers owned by the individuals, or those owned by research projects of the faculty, when connected to campus network are subjected to comply all steps mentioned guidelines. Further, all the faculty, students, staff, departments, authorized visitors/visiting faculty and others who will be granted permission to use the University's information technology infrastructure, must comply with the Guidelines.

Violations of any guideline by any university member will result in disciplinary action against the offender by the university authorities. If the matter involves illegal action, the case may be referred to appropriate law enforcement agency.

The revised IT policy is classified into following groups:

- IT Services
- IT Hardware and Software Installation & Licensing
- Open Source Resource Usage
- Network and Information Security
- Green Computing
- Wi-Fi access usage

Further, the policies will be applicable at two levels:

- End Users Groups (Faculty, students, Senior administrators, Officers and other staff)
- Network Administrators

IT Services

Enhanced E-Governance Services

The University already started few online services for students such as online fees submission, registration and exam form submission. However, University Management Software, an ERP software is yet to be implemented. IT Centre has taken initiative to develop University Management Software for providing enhanced online services to students, MIS services to university administration and online services to other stakeholders.

Smart ID Card Usage

All users will have single smart card based ID, for all the university services and authentications. This will promote e-governance and forming a digital university.

Extension and field Outreach Plan

- Extending University IT services and resources to the remote affiliated colleges and other institutions like Gram Panchayats, by providing them remote connectivity.
- Developing video-conferencing facilities to deliver higher education to the residents of rural areas at affordable cost.

Wireless Infrastructure and Applications:

Enhance the wireless network access in the campus for all offices, buildings, hostels and open-access areas. Integration of university services on handheld devices to enhance communications among university members. As portable hand-held devices are becoming more powerful, we shall explore and provide the necessary infrastructure to support new mobile applications to allow University members to use their hand-held devices with built-in browsers to access information anytime and anywhere in the university.

IP Telephony to Integrate Data, Voice and Video Deliveries

This saves cost on cabling and relocation of phone lines from one location to another. Our campus network infrastructure has the necessary coverage, bandwidth, resiliency and security to support IP telephony.

Data Resource Centre for e-Governance

Acting as a data resource Centre for e-Governance services and collaborate with Government agencies.

Test Bed for Experimental Research

Creation of test bed facilities for experimental research in areas like wireless sensor networks, multimedia networks and pervasive computing.

IT Hardware, Software Installation and Licensing

University network user community will have to observe certain precautions while getting their computers or peripherals installed so that he/she may face minimum inconvenience due to interruption of services due to hardware failures. The important and mandatory steps to be followed at IT hardware installation are:

- If the computer is installed in a room and used by an individual is designated as single/personal user. If a computer is used by a group of multiple users, then the department Head will designate a person from that group responsible for compliance. The University will consider server(s) not directly administered by IT Centre as end user computers.
- The procured hardware must comply applicable quality standards. The hardware installation and configuration must be done by following set norms and procedures.
- Necessary power conditioning, which includes electrical earthing and stabilized power should be done before any hardware installation.
-

- The University IT policy does not allow any pirated/unauthorized software installation on the university owned computers and the computers connected to the university campus network.

a) Warranty & Annual Maintenance Contract

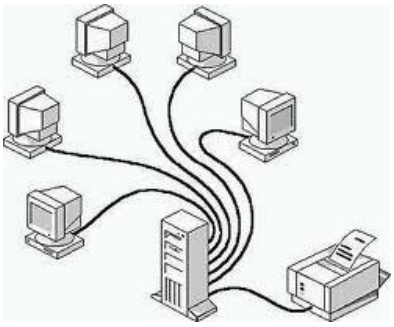
The Computers or any networking equipment purchased by any Department will be preferably with minimum 3-year on-site comprehensive warranty. These equipments must be covered under annual maintenance contract after the expiry of warranty.

c) Network Cable Connection

While connecting the computer or peripheral to the network, the connecting network cable should be away from any electrical/electronic equipment, as they interfere with the network communication. Further, no other electrical/electronic equipment should be shared with the power supply from where the computer and its peripherals are connected.

d) File and Print Sharing Facilities

File and print sharing facilities on the computer over the network to be installed only when it is absolutely required. When files are shared through network, they should be protected with password and also with read only access rule.



e) Noncompliance

DAVV faculty, staff, and students not complying with this computer hardware installation policy will leave themselves and others at risk of network related problems,

which could result in damaged or lost files, inoperable computer resulting in loss of productivity. Such computers will not be permitted for network connection.

Any computer purchases made by the individual departments/projects will be with necessary licensed software (operating system, antivirus software and necessary application software) installed. Respecting the anti-piracy laws of the country, The University IT policy does not allow any pirated/unauthorized software installation on the university owned computers and the computers connected to the university campus network. In case of any such instances, university will hold the department/primary user personally responsible for any pirated software installed on the computers located in their department/individuals' rooms. Preference will be given to install and use open source software products wherever it is applicable.

a) Operating System and its Updating

Single/personal users to make sure that respective computer systems install updated operating system with respective service packs/patches, particularly with Windows based OS. Latest service packs/patches help in fixing bugs and vulnerabilities in the OS that were periodically detected by the Microsoft. Free OS updates are available on official website of company. It will be user's responsibility to go for updates regularly, preferably once in a week. University

encourages the use of open source software such as Linux, Open office wherever possible.

b) Antivirus Software and its Updating

All Computer systems used in the university will have anti-virus software installed, and it should be active at all times. The single/personal user of a computer system will be responsible for keeping the computer system compliant with this virus protection policy.

Individual users should make sure that respective computer systems have current virus protection software installed and maintained and it should be running correctly. The antivirus software that is running on a computer must be either obtained from centrally purchased in IT Center or it should be procured at department level. The software subscription must be regularly renewed.

c) Backup of Data

Users should perform regular backups of their vital data. Virus infections often destroy data on an individual's computer. Without proper backups, recovery of destroyed files may be impossible. At the time of OS installation, it is advised that the computer's hard disk partitioned into two volumes typically C and D. OS and other software should be on C drive and user's data files on the D drive. In case of any virus problem, generally only C volume gets corrupted. In such an event formatting only one volume, will protect the data loss. However, it is not a foolproof solution. Apart from this, users should keep their valuable data on suitable backup device such as Floppy, CD or pen drives.

d) Noncompliance

DAVV faculty, staff, and students not complying with this software installation policy will leave themselves and others at risk of virus infections which could result in damaged or lost files inoperable computer resulting in loss of productivity at individual, department or even at University level. Such computer users will be notified time to time and will be advised and given help to follow correct steps.

IT Centre Interface

IT Centre upon finding a non-compliant computer affecting the network, will notify the individual responsible through respective head of department for the system and ask that it be brought into compliance. Such notification will be done via email/telephone. The individual users will follow-up the notification to be certain that his/her computer gains necessary compliance. The IT Centre will provide guidance as needed for the individual to gain compliance.

Open Source Resource Usage

The University has always followed the policy of providing IT services to its users strictly using open source operating system platforms. Hence all its servers are using different flavors of Linux operating system and open source tools available on this platform. IT centre since its inception has promoted the usage of Linux OS in server room. IT Center will always provide technical support to other departments who are willing to use open source software.

Network and Information Security

The campus wide Network connectivity provided through the University, referred to hereafter as "the Network", either through an authenticated network access connection or a Virtual Private Network (VPN) connection will be governed under the University IT Policy. The IT Centre will be coordinating for the ongoing maintenance and support of the Network, exclusive of local applications. Problems within the University's network will be reported to IT Centre by departments. IT Centre will rectify reported problems and ensure seamless network connectivity.

a) IP Addressing Scheme

IT Centre has already formulated an IP addressing scheme. In this addressing scheme each UTD is allocated a pool of private IP addresses. IT Centre will maintain central DHCP server for dynamic IP address allocation for individual computers. Any computer in a UTD connected to the university network will have IP address only from an address pool assigned to that UTD.

b) DHCP and Proxy Configuration by Individual Departments /Users

Use of any computer at end user location as a DHCP server to connect to more computers through an individual switch/hub and distributing IP addresses (public or private) should strictly be avoided, as it is considered absolute violation of IP address allocation policy Connecting wireless access point(s) at end user location and using multiple computers should not be permitted. Similarly, configuration of proxy servers should also be avoided, as it may interfere with the service run by IT center. Non-

compliance to the IP address allocation policy will result in disconnecting the port from which such computer is connected to the network.

Connection will be restored after receiving written assurance of compliance from the concerned department/user.

c) Running Network Services on the Servers

Individual departments/individuals connecting to the university network over the LAN may run server software, e.g., HTTP/Web server, SMTP server, FTP server, only after bringing it to the knowledge of the IT Center in writing and after meeting the requirements of the university IT policy for running such services. Non-compliance with this policy will be treated direct violation of the university IT policy. This will result in termination of their connection to the Network. IT Center takes no responsibility for the content of machines connected to the Network, regardless of those machines being University or personal property. IT Center will be constrained to disconnect client machines where potentially damaging software is found to exist. A client machine may also be disconnected if the client's activity adversely affects the Network's performance.

Access to remote networks using a University's network connection must be in compliance with all policies and rules of those networks. This applies to any and all networks to which the University Network connects. University network and computer resources are not to be used for personal commercial purposes. Network traffic will be monitored for security and for performance reasons at IT Center. Impersonation of an authorized user while connecting to the Network is in direct violation and will result in the termination of the connection.

d) Dial-up/Broadband Connections

End user computer systems that are part of the University's campus-wide network, whether university's property or personal property, should not be used for dial-up/broadband connections, as it violates the university's security by way of bypassing the firewalls and other network monitoring servers. Non-compliance with this policy may result in withdrawing the IP address allotted to that computer system. Departments already having broadband connections should inform IT center about public/private IP addresses they are using and they must take utmost care to prevent any unauthorized access in the network.

e) Wireless Local Area Networking

University is having policy of controller based campus wide Wi-Fi network and further, it is to be extended within academic buildings. The campus Wi-Fi network is centrally managed by IT Center. Each wireless access point as well as end user mobile device connected in Wi-Fi network must be registered with IT Center including point of contact information. This policy applies to users of all UTDs and other sections of university.

School, departments, or divisions must not operate wireless local area networks with unrestricted access. Network access must be restricted either via authentication or MAC/IP address restrictions. Passwords and data must be encrypted.

f) Internet Bandwidth obtained by Other Departments

Internet bandwidth obtained by any School/Centre, department of the university under any research program/project should ideally be pooled with the university's Internet bandwidth, and be treated as university's common resource. Under particular circumstances, which prevent any such pooling with the university Internet bandwidth, such network should be totally separated from the university's campus network. These networks should use separate IP addressing scheme and should take necessary network security measures in accordance to university IT policy. The network details which include network design and the IP address schemes may be submitted to IT Center. Non-compliance to this policy will be direct violation of the university's IT security policy.

g) Email Account Use Policy

University IT Center has installed e-mail service for its faculty, staff and university administrators with url: http://mail.dauniv.ac.in . It is recommended to utilize this e-mail service for academic and official communication. Formal official notices to faculty and staff may also be circulated through this service. E-mail service will facilitate fast delivery of messages and documents to campus and external user groups or individual users. The user may contact IT center for e-mail account and default password. The e-mail address should be kept active by using it regularly. Users using e-mail facility will be agreeing to abide following:

i) Facility will be used for academic and official purposes only. Use of this facility for commercial or illegal purposes is direct violation of university's IT policy and may subject to withdrawal of the facility. Illegal use includes but not limited to, sending the unlicensed and illegal software as attachment,

unsolicited bulk e-mail messages and generation of threatening, harassing, abusive, obscene or fraudulent messages/images.

ii) User should keep the mail box used space within about 80% usage threshold, as 'mail box full' or 'mailbox all most full' situation will result in bouncing of the mails, especially when the incoming mail contains large attachments.

iii) User should not open any mail or attachment that is from unknown and suspicious source, such messages may contain viruses that have potential to damage the valuable information on your computer.

iv) It is user's responsibility to keep a backup of the incoming and outgoing mails of their account. User should not share his/her email account and password with others, as the individual account holder is personally held accountable, in case of any misuse of that email account.

v) User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.

vi) Impersonating email account of others will be taken as a serious offence under the university IT security policy.

vii) Any Spam mail received by the user into INBOX should be forwarded to spam@mail.dauniv.ac.in. Any mail wrongly stamped as SPAM mail should be forwarded to wrongspam@mail.daunic.ac.in.

Software Asset Management

The University promotes the policy of using licensed software on its network. All purchased computers use licensed operating system and tools. The software purchase is done in centralized or departmental level. Any software will be purchased either with perpetual licenses or on annual subscription basis.

The old software must be upgraded with higher version for enhanced features or better performance. The subscription renewal or version up gradation of software will be done at department level or through IT Center whichever is applicable. IT Centre will normally use enterprise level operating system and UTM and antivirus software. The subscription for software needs to be renewed on annual basis. IT Centre will centrally manage the renewal of such subscriptions.

Green Computing

University has commitment in maintaining and improving on the "Green Ethos" in the campus. It is a continuing process of review and exploration of improving technologies and practices.

Our core green computing policy objectives are to:

- Benefit the environment by conserving resources
- Reduce e-waste
- Reduce costs through efficiencies and staff awareness
- Promote purchase of ICT infrastructure from the green certified suppliers
- Improve stakeholder awareness of "Green IT Issues"

These objectives will be achieved through the following guide lines and actions:

- Look at power consumption and reduction in power consumption when upgrading ICT hardware.
- Investigate carbon offset programs to offset ICT carbon emissions.
- Promote the policy of using server virtualization concept.

- A compulsory manufacturer takes back policy, taking into consideration the use of Hazardous Substances in Electrical and Electronic Equipments. This requires ICT manufacturers to take back old ICT hardware when new hardware is purchased or upgraded.
- Promote Star Energy/EPEAT/TCO energy efficient rating system in purchase of ICT and electronic goods. This will allow ICT professionals to compare the energy consumption of ICT products and make the best choice in terms of reducing energy use and costs.

Concluding Remarks

The purpose of this IT policy is to tell its users about various IT service commitments from University. It will also guide users and IT resource administrators on issues related to the proper and ethical use of technology and information in their organization. This document also gives future plan If something which is unlawful and is not specified explicitly in the policy as illegal or unauthorized, it may still be considered as breach of the university rules and provisions made in IT act. One should use own wisdom and critical thinking in handling such situations.

****

UNIVERSITY IT POLICY

CONCEPTUALISED AND FRAMED BY:

IT CENTRE AND

COMPUTER CENTRE

PUBLISHED BY:

REGISTRAR

DEVI AHILYA VISHWAVIDYALAYA, INDORE